

INTERTRA NETWORKS – ROBOCALL MITIGATION PLAN

1. Company Overview

Interra Networks provides enterprise voice services and managed call-center solutions. Interra originates outbound voice traffic for business and public-sector clients but does not operate as an intermediate or terminating voice service provider. All outbound SIP traffic is delivered through fully STIR/SHAKEN-compliant upstream carriers.

2. STIR/SHAKEN Compliance

- Interra Networks' outbound calls are signed with authenticated caller identity information by compliant upstream carriers.
 - Interra does not currently operate its own STIR/SHAKEN authentication service but ensures all traffic remains within STIR/SHAKEN-enabled IP networks.
 - Interra requires all carrier partners to maintain valid STIR/SHAKEN certification and to block or challenge unauthenticated calls.
-

3. Know-Your-Customer (KYC) Controls

Interra uses a strict onboarding and verification process:

✓ Identity Verification

Business registration documents, government ID for authorized representatives, tax ID, and physical address validation.

✓ Use-Case Review

Clients must declare:

- Type of calls (customer service, public health, verification, etc.)
- Calling lists and opt-in methods

- Caller ID numbers used
- Consent collection procedures

✓ High-Risk Caller Screening

Interra rejects:

- Lead-generation robocallers
 - Auto-dialed marketing campaigns without documented consent
 - Any client failing verification checks
-

4. Caller ID Authentication & Accuracy Measures

- All caller ID numbers used by clients must be verified as owned or legally authorized.
 - Unauthorized or unverifiable caller IDs are rejected.
 - Spoofing of numbers without permission is strictly prohibited.
-

5. Ongoing Traffic Monitoring

Interra uses analytics and pattern-based monitoring to detect illegal or suspicious calling behavior:

Real-time monitoring includes:

- High-volume short-duration calls
- Flash-burst call patterns
- Calls to numbers on known Do-Not-Call or fraud lists
- Sudden changes in traffic profile
- Unexpected spikes in call attempts

If suspicious activity is detected, Interra will:

1. Alert the customer immediately
2. Investigate the traffic
3. Suspend or block calling if needed to prevent potential illegal robocalls

6. Robocall Prevention & Blocking Protocol

Interra will block traffic if:

- Caller ID is invalid
- The calling pattern appears malicious or in violation of FCC rules
- The client fails to provide proof of consent for high-volume/automated campaigns
- The ITG or FCC notifies Interra of suspected illegal robocalling

7. Cooperation With the Industry Traceback Group (ITG)

Interra Networks will:

- Respond to traceback requests within **24 hours**
- Provide all necessary records for identifying upstream sources of illegal calls
- Immediately restrict or terminate clients involved in violating traffic

This satisfies the FCC's mandatory traceback response requirement.

8. Employee Training

All operations and network teams are trained on:

- FCC robocall rules
- Caller ID authentication
- Traffic monitoring and identification of violations
- Emergency shutdown procedures

9. Enforcement & Corrective Action

If a customer is suspected of illegal robocalling:

1. Traffic is temporarily halted

2. The customer must provide evidence of permission/consent
 3. Violators are permanently terminated
 4. Relevant evidence will be provided to law enforcement or regulators
-

10. Commitment to Compliance

Interra Networks certifies:

- Its robocall mitigation protocols meet FCC requirements
- It will maintain accurate filings in the Robocall Mitigation Database
- It will continuously monitor traffic and enforce compliance